**ПРОГРАММА КУРСА**

**Цифровые технологии**

*(1/2 года, лектор проф ЮВ Нестеренко, приглашаются студенты 1-6 курсов.*

*Лекции будут читаться дистанционно в Zoom.*

*Идентификатор конференции 322 972 5298, код доступа 314159 )*

1. **Алгоритмы и сложность.**
   1. Алгоритм Евклида и теорема Ламе.
   2. Символы Лежандра и Якоби.
   3. Возведение в степень.
   4. Быстрое умножение целых чисел.
   5. Вероятностные методы отсеивания составных чисел.
   6. Доказательство простоты больших чисел. Последовательности псевдослучайных чисел. Линейный конгруэнтный метод. Хеш-функции и псевдослучайные последовательности.
   7. Первообразные корни и дискретное логарифмирование.
   8. Задача разложения целых чисел на множители. Алгоритм пробных делений.

ρ — метод Полларда.

* 1. Эллиптические кривые. Метод касательных и секущих. Сложение точек на эллиптической кривой Эллиптические кривые над конечными полями

1. **Криптографические примитивы**
   1. Алгоритм Диффи-Хеллмана обмена ключами
   2. Алгоритм RSA
   3. Хеш-функции
      1. Логические операции
      2. Символы и операции
      3. Функции и константы
      4. Предварительная подготовка
      5. Алгоритм хеширования SНА-256

Криптография с открытым ключом. Шифрование RSА (продолжение). Криптосистемы Эль-Гамаля и Рабина.

1. **Информационные технологии**
   1. Электронная подпись. Подписи Шнорра, DSA (Digital Signature Algorithm), RSA. Электронная подпись с помощью эллиптических кривых.
   2. Схемы обязательств.
   3. Подтверждение выбора (Доказательство с нулевым разглашением).
   4. Разделение секрета.
   5. Протокол аутентификации.

3.6. Система электронного голосования.

3.7. Технологии блокчейн.

3.8. Криптовалюта – биткойн.